What is claimed is:

1. A single sign-on computer system comprising:

(a) a client device capable of communicating with a server network;

(b) a server network, the server network comprising:

an account collaboration agent server, the account collaboration agent server in communication with the client device;

at least one web server for accessing at least one associated target web-based application, the at least one web server having an associated time clock, and wherein the at least one web server is in communication with the account collaboration agent server;

at least one database server associated with the at least one web server, the at least one database server in communication with the at least one web-server and in further communication with the account collaboration agent server; and

(c) means for securely defining a user profile, the user profile capable of being retrieved by the account collaboration agent server.

2. The single sign on system of claim 1 wherein the account collaboration agent server further comprises memory means for securely storing the user profile there within.

3. The single sign on system of claim 1 wherein the account collaboration agent server further comprises:

(a) means for securely retrieving the user profile from the memory means, wherein the user profile comprises a user identification and an associated user password;

(b) means for building a secure connection string between the client device and the server network;

(c) means for timing an amount of time a user accesses the single sign on system, the means for timing comprises a clock counter, and wherein the clock counter initializes and begins counting the time once the user profile is retrieved from the user profile memory means, and stops counting once a user having the associated user profile logs off of the single sign on system;

(d) means for synchronizing the clock counter with the at least one web server time clock;

(e) at least one session variable index register for indexing a user's session variables, the session variables comprise an authenticated and authorized user identification and a timestamp associated with the user identification, the timestamp is an indicated time value extracted from the clock counter when an authenticated and authorized user requests access to the at least one web server target application; and

(f) means for defining a database schema, wherein the schema allows secure communications between the account collaboration agent server, the at least one web server, and the associated at least one server database.

4. The single sign on system of claim 3 wherein the means for defining a database schema further comprises an account collaboration program for executing control over the session variables to securely communicate the session variables from the account collaboration agent server to the at least one web-based server when a user requests access to the at least one web-based server.

5. The single sign on of claim 4 wherein the an account collaboration program is replicated in the at least one web server.

6. The single sign on of claim 3 wherein the at least one database has a user identification index register stored within for indexing the user identification.

7. A single sign-on computer system comprising:

(a) a client device capable of communicating with a server network;

(b) a server network, the server network comprising:

at least a first web server for accessing at least one first associated target web-based application, the at least first web server having an associated first database server in communication with the at least one first web server, and wherein the at least one web server has an associated first time clock,

at least a second web server for accessing at least one second associated target web-based application, the at least one second web server having an associated second database server in communication with the at least one second web server, and wherein the at least one web server has an associated second time clock,

an account collaboration agent server in communication with the client device, the first web server, and the second web server, the account collaboration agent server comprises:

means for securely retrieving a user profile, wherein the user profile comprises a user identification and an associated user password,

means for building a secure connection string between the client device and the server network,

means for timing an amount of time a user accesses the single sign on system, the means for timing comprises a clock counter, and wherein the clock counter initializes and begins counting the time once the user profile is accessed, and stops counting once a

user having the associated user profile logs off of the single sign on system,

means for synchronizing the clock counter with the at least two web servers time clocks;

at least one session variable index register for indexing a user's session variables, the session variables comprise an authenticated and authorized user identification and an initial timestamp associated with the user identification, the initial timestamp is an indicated time value extracted from the clock counter when an authenticated and authorized user requests access to the at least one web server target application, and

means for defining a database schema, wherein the schema allows secure communications between the account collaboration agent server, the at least two web servers, and their associated at least two server databases; and

(c) means for defining a user profile, the user profile capable of being retrieved by the account collaboration agent server.

8. The single sign on system of claim 7 wherein the account collaboration agent server further comprises memory means for securely storing the user profile there within.

9. The single sign on system of claim 8 wherein the means for defining a database schema further comprises an account collaboration program for executing control over the session variables to securely communicate the session variables from the account collaboration agent server to the at least one web-based server when a user requests access to the at least one web-based server.

10. The single sign on of claim 9 wherein the an account collaboration program is replicated in the at least two web servers.

11. The single sign on of claim 9 wherein the at least first associated database has a first web-server session variable index register for indexing a users first web-server session variables, the first session variables comprise an authenticated and authorized user identification and an associated first web-server timestamp, the associated first web-server timestamp is an indicated first time variable extracted from the first web server time clock when an authenticated and authorized user requests access to the at least second web server target application.

12. The single sign on of claim 9 wherein the at least second associated database has a second web-server session variable index register for indexing a users second web-server session variables, the second session variables comprise an authenticated and authorized user identification and an associated second web-server timestamp, the associated second web-server timestamp is an indicated second time variable extracted from the second web server time clock when an authenticated and authorized user requests access to the at least first web server target application.

13. A method of using the single sign on system of claim 11 comprising the steps of logging a user into the single sign on system; building a secure connection string between the account collaboration agent server and the client device; synchronizing the account collaboration agent server counter clock with the at least first and second time clocks associated with the at least two web servers; defining the database schema; securely logging into the at least first target web application; securely logging onto the at least second target web application after first logging into the first target web application.

14. The method of claim 13 wherein the step of securely logging into the second target application further comprises executing the account collaboration agent server program upon sending a log-on request from the at least first web server to the at least second web server; extracting the user identification and associated first timestamp from the at least first web server session variable index at the same time the sent log-on request to the second web server is sent; storing the extracted first web server variables within the second web database; comparing the

received extracted user identification variable sent from the first web server with the user identification variable stored in the second web server session variable index; denying access to the second web server if the received extracted user identification does not match the stored second web server user identification variable; clearing the first web server time stamp from the first web server session variable index; comparing the extracted first web server timestamp with a time indicated on the second server time clock; denying access to the second web application if the extracted timestamp and the indicated time on the second server time clock is greater than n seconds; allowing access to the second web application if the extracted timestamp and the indicated time on the second server time clock is equal to or less than n seconds; and clearing extracted first web time stamp variable stored within the second web database.

15. The method of claim 14 wherein n equals three seconds.

16. The method of claim 15 wherein the step of securely logging into the first target application further comprises: executing the account collaboration agent server program upon sending a log-on request from the at least second web server to the at least first web server; extracting the user identification and associated second timestamp from the at least second web server session variable index at the same time the sent log-on request to the first web server is sent; storing the extracted second web server variables within the first web database; comparing the received extracted user identification variable sent from the second web server with the user identification variable stored in the first web server session variable index; denying access to the first web server if the received extracted user identification does not match the stored first web server user identification variable; clearing the second web server time stamp from the second web server session variable index; comparing the extracted second web server timestamp with a time indicated on the first server time clock; denying access to the first web application if the extracted timestamp and the indicated time on the first server time clock is greater than n

seconds; allowing access to the first web application if the extracted timestamp and the indicated time on the first server time clock is equal to or less than n seconds; and clearing extracted second web time stamp variable stored within the first web database.

17. The method of claim 16 wherein n equals three seconds.